REMARKS

CLAIMS

For nearly all of the claims presented in the present Application, the Applicants have noticed that the Office Action has simply referenced paragraph numbers of one or more of the cited references in an attempt to show a teaching of the one or more elements and/or features recited in the claims. For example, the Office Action alleges that one or more paragraphs in a cited reference teaches what is recited in a claim without specifically showing how the cited references teach each and every element and/or feature of that claim. Applicants respectfully submit that the Office Action must clearly show out how each and every element and/or feature of what is recited in each claim is taught by the cited references. Otherwise, the claim should be advanced to allowance. In general, the Applicants feel that the Office Action has not shown a teaching of each and every element and/or feature of the claims of the present Application. Applicants believe that the elements and/or features recited in Claims 1-22 are novel and should be passed to issue.

REJECTION OF CLAIMS 1-6, 14-16, AND 20-22 UNDER 35 U.S.C. § 102(e)

Claims 1-6, 14-16, and 20-22 are rejected under 35 U.S.C. 102(e) as being anticipated by Gressel et al. (2004/0205095 Al). Regarding independent Claim 1, the Office Action states:

> Regarding claim 1, Gressel et al. teaches a method of generating pseudo-random numbers using a linear feedback shift register (0044-0046, 0026 and 0098) in which the correlation between successive pseudo-random numbers is reduced (0046), said method comprising sampling output sequences of said linear feedback shift register with a specified periodicity (0096, 0046, abstract, 0026-0027, and 0097).

See Office Action at page 2.

Independent Claim 1 recites "a method of generating pseudo-random numbers using a linear feedback shift register in which the correlation between successive pseudo-random numbers is reduced, said method comprising sampling output sequences of said linear feedback shift register with a specified periodicity." The Office Action alleges that Gressel, at paragraph 0046 teaches "in which the correlation between successive pseudo-random numbers is reduced," as recited in Claim 1. After reviewing Gressel, at paragraph 0046, the Applicants do not see how this paragraph discloses what is recited in Claim 1. Nowhere is there any mention of any of the elements and/or features of "in which the correlation between successive pseudo-random numbers is reduced." Therefore, for this reason alone, the Applicants respectfully submit that the Office Action has not shown a teaching of what is recited in independent Claim 1. As a consequence, the Applicants believe that Claim 1 contains patentable subject matter.

The Office Action further alleges that Gressel, at paragraphs 0096, 0046, abstract, 0026-0027, and 0097, teaches a "method comprising sampling output sequences of said linear feedback shift register with a specified periodicity," as recited in Claim 1. After reviewing paragraph 0096, 0046, abstract, 0026-0027, and 0097, the Applicants do not see how these paragraphs disclose the elements and/or features recited in this portion of Claim 1. Therefore, for this reason alone, the Applicants respectfully submit that the Office Action has not shown a teaching of what is recited in independent Claim 1. As a consequence, the Applicants believe that Claim 1 contains patentable subject matter.

The Applicants would like to provide an argument that supports the patentability of Claim 1 by, referencing paragraph 0043 of Gressel, which states:

> All of the embodiments are based on the logic of randomly distorted pseudorandom binary sequences, as produced by maximum length linear feedback shift registers, (LFSRs). These sequences may be produced in a compact form using LFSRs with glue logic, which distorts the sequences by changing the stage of the register in a given sequence at *random periods*, and/or by changing the feedback taps in an LFSR, which quickly changes the sequence produced by clocking the LFSR.

As indicated in 0043, "the sequences may be produced in a compact form using LFSRs with glue logic, which distorts the sequences by changing the stage of the register in a given sequence at *random periods*, and/or by changing the feedback taps in an LFSR, which quickly changes the sequence produced by clocking the LFSR." (emphasis denoted in italics). Thus, based on what Gressel discloses in paragraph 0043, Gressel does not teach or disclose "sampling output sequences of said linear feedback shift register with a specified periodicity," as recited in Claim 1. Thus, for this reason alone, Gressel does not teach what is recited in the claimed invention. Consequently, the Applicants respectfully submit that the Office Action has not shown a teaching of what is recited in independent Claim 1. As a consequence, the Applicants respectfully submit that Claim 1 contains patentable subject matter.

If the Examiner wishes to maintain the rejection to Claim 1, the Applicants respectfully request that the Examiner should clearly show how each and every element of Claim 1 is taught by Gressel. Otherwise, the Applicants respectfully submit that independent Claim 1 contains patentable subject matter; and as a consequence, Claim 1 should be allowed.

As a result of providing the foregoing arguments with respect to independent Claim 1, the Applicants have not commented on the remarks made by the Examiner regarding dependent Claims 2-6, 14-16, and 20-22, but reserve the right to do so in the future should the need arise.

Since Claims 2-6, 14-16, and 20-22 depend on allowable Claim 1, the Applicants respectfully submit that Claims 2-6, 14-16, and 20-22 are in condition for allowance. The Applicants respectfully request allowance of Claims 1-6, 14-16, and 20-22.

REJECTION OF CLAIMS 7-10 and 19 UNDER 35 U.S.C. § 102(e)

Claims 7-10 and 19 are rejected under 35 U.S.C. 102(e) as being anticipated by Furuta et al. (5327522). Regarding independent Claim 7, the Office Action states:

> Regarding claim 7, Furuta et al. teaches a method of generating pseudo-random numbers using linear feedback shift registers (col. 44 lines 55-68) in which the correlation between successive pseudo-random numbers is reduced (col. 67 lines 36-col. 68 lines 2), said method comprising periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register (col. 67 lines 36-col. 68 lines 2).

See Office Action at pages 3-4.

Independent Claim 7 recites "a method of generating pseudo-random numbers using linear feedback shift registers in which the correlation between successive pseudo-random numbers is reduced, said method comprising periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register." The Office Action alleges that col. 67, line 36 – col. 68, line 2 of Furuta teaches "in which the correlation between successive pseudo-random numbers is reduced, said method comprising periodically switching between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register," as recited in independent Claim 7. After reviewing col. 67, line 36 – col. 68, line 2 of Furuta, the Applicants do not see how this passage discloses what is recited in Claim 7. Nowhere is there any mention of "*periodically switching* between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register," as recited in Claim 7. While Furuta may disclose that without Furuta's switching circuitry (i.e., 1309 in Figure 126), "random pulses will be repeated periodically if this connection is fixed," Furuta does not disclose anything about "*periodically switching* between iterative outputs generated by at least a first linear feedback shift register and iterative outputs generated by at least a second linear feedback shift register," as recited in Claim 7. Thus, Furuta does not teach what is recited in Claim 7. Consequently, the Applicants respectfully submit that the Office Action has not shown a teaching of what is recited in independent Claim 7. As a consequence, the Applicants believe that Claim 7 contains patentable subject matter.

If the Examiner wishes to maintain the rejection to Claim 7, the Applicants respectfully request that the Examiner should clearly show how each and every element of Claim 7 is taught by Furuta. Otherwise, the Applicants respectfully submit that independent Claim 7 contains patentable subject matter; and as a consequence, Claim 7 should be allowed.

With respect to dependent Claims 9-10, the Office Action alleges "Furuta et al. teaches the method wherein said pseudo-random numbers are generated with period equal to the sum of each of the individual linear feedback shift register periods (col. 47 lines 47-col. 48 lines 15)." While Furuta may disclose a "logical sum of pulse densities," nowhere does Furuta disclose a "period equal to the sum of each of the individual linear feedback shift register periods," as recited in Claims 9-10. Thus, the Examiner has not shown a teaching of what is recited in Claims 9-10. For this reason alone, the Applicants respectfully submit that Claims 9-10 contain patentable subject matter. As a consequence, dependent Claims 9-10 should be allowed.

As a result of providing the foregoing arguments with respect to independent Claim 7, the Applicants may not have commented on all the remarks made by the Examiner regarding dependent Claims 8-10 and 18-19, but reserve the right to do so in the future should the need arise. Since Claims 8-10 and 18-19 depend on allowable Claim 7, the Applicants respectfully submit that Claims 7-10 and 18-19 are in condition for allowance. The Applicants respectfully request allowance of Claims 7-10 and 18-19.

REJECTION OF CLAIMS 11-13 UNDER 35 U.S.C. § 102(e)

Claims 11-13 are rejected under 35 U.S.C. 102(e) as being anticipated by Thomas et al. (2003/0072059 Al). Regarding independent Claim 11, the Office Action states:

> Regarding claim 11, Thomas et al. discloses a method of encrypting a pseudo-random number (claim 3) generated by a linear feedback shift register (par. 0146 and claim 35) comprising operating a nonlinear operator on said pseudo-random number and one or more operands (claim 29, and par. 0213, and 0155).

See Office Action at pages 4-5.

Independent Claim 11 recites "a method of encrypting a pseudo-random number generated by a linear feedback shift register comprising operating a nonlinear operator on said pseudo-random number and one or more operands." After reviewing Thomas, at Claim 29, and paragraphs 0213 and 0155, the Applicants do not see how Claim 29 or these paragraphs disclose what is recited in Claim 11. Nowhere is there any mention of any of the elements and/or features of "operating a nonlinear operator on said pseudo-random number and one or more operands." For example, paragraph 0155 discloses "a submethod 905 for generating non-linear filtered output bits from shift registers." A method for generating non-linear filtered output bits does not teach "operating a nonlinear operator on said [a] pseudorandom number and one or more operands." Furthermore, Thomas, at paragraph 0213, discloses generating "a key stream from feedback taps in a non-linear matter" which is different from "operating a nonlinear operator on said [a] pseudorandom number and one or more operands." Neither paragraph even discloses the feature of "operating a nonlinear operator" as recited in Claim 11. To further clarify, Thomas, at Claim 29, discloses an output between a first tap and a second tap comprising a non-linear value. The non-linear value is an output which is not a "nonlinear operator," as recited in Claim 11. Therefore, for each of these reasons individually, the Applicants respectfully submit that the Office Action has not shown a teaching of what is recited in independent Claim 11. As a consequence, the Applicants believe that Claim 11 contains patentable subject matter.

If the Examiner wishes to maintain the rejection to Claim 11, the Applicants respectfully request that the Examiner should clearly show how each and every element of Claim 11 is taught by Thomas. Otherwise, the Applicants respectfully submit that independent Claim 11 contains patentable subject matter; and as a consequence, Claim 11 should be allowed.

As a result of providing the foregoing arguments with respect to independent Claim 11, the Applicants may not have commented on all the remarks made by the Examiner regarding dependent Claims 12-13, but reserve the right to do so in the future should the need arise. Since Claims 12-13 depend on allowable Claim 11, the Applicants respectfully submit that Claims 12-13 are in condition for allowance. The Applicants respectfully request allowance of Claims 11-13.

REJECTION OF CLAIM 17 UNDER 35 U.S.C. § 102(e)

Claim 17 is rejected under 35 U.S.C. 102(e) as being anticipated by Walmsley 20050066168 Al. Regarding independent Claim 11, the Office Action states:

> Regarding claim 17, Walmsley discloses a method of further encrypting a pseudo-random number (par. 0338, 0344, and 0358) generated from a linear feedback shift register (fig. 9) by using a hashing function (0771, and 0774-0775) comprising: receiving said pseudo-random number generated from said linear feedback shift register (0358-0365 and 0942-0934); and varying the initial value of said hashing function over time by way of a function operating on one or more variables (0358-0365 and 0942-0934).

See Office Action at pages 4-5.

Claim 17 recites "A method of further encrypting a pseudo-random number generated from a linear feedback shift register by using a hashing function comprising receiving said pseudo-random number generated from said linear feedback shift register, and varying the initial value of said hashing function over time by way of a function operating on one or more variables." The Office Action references paragraphs 0942-0934 [sic]. It appears that the Office Action contains a typographical error. The Applicants have interpreted the Office Action as referencing paragraphs 0942-0943. After reviewing Walmsley, at 0358-0365 and 0942-0943, the Applicants do not see how these paragraphs disclose what is recited in Claim 17. Nowhere is there any disclosure of any of the elements and/or features of "varying the initial value of said hashing function over time by way of a function operating on one or more variables," as recited in Claim 17. For example, paragraphs 0358-0365 and 0942-0934 do not disclose anything about an "initial value of said hashing function." For each of these reasons, the Applicants respectfully submit that the Examiner has not shown a teaching of what is recited in independent Claim 17.

If the Examiner wishes to maintain the rejection to Claim 17, the Applicants respectfully request that the Examiner should clearly show how each and every element of Claim 17 is taught by Walmsley. Otherwise, the Applicants respectfully submit that independent Claim 17 contains patentable subject matter; and as a consequence, Claim 17 should be allowed.

REJECTION OF DEPENDENT CLAIM 18 UNDER 35 U.S.C. § 103(a)

It appears that the Office Action is in error when it states that "*Claim 19* [18] is rejected under 35 U.S.C. 103(a) as being unpatentable over Furuta et al. (5327522) in view of Gressel et al. 2004/0205095 Al." The Applicants believe that Examiner's reference to Claim 19 is a typographical error since the Examiner's argument subsequently refers to Claim 18. Therefore, the Applicants will address a response to Claim 18.

Regarding Claim 18, the Office Action states:

> Regarding claim 18, Furuta et al. teaches the method further comprising: receiving said pseudo-random number generated from said linear feedback shift register (col. 44 lines 55-68); Furuta et al. fails to varying the initial value of said hashing function over time byway of a function operating on one or more variables. However Gressel et al. discloses receiving said pseudo-random number generated from said linear feedback shift register (0148, 0156); and varying the initial value of said hashing function over time by way of a function operating on one or more variables (0183, 0197, 0372, and 0455). Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to combine the teachings because they are analogous in LFSR random number generation. One would have been motivated to incorporate the teachings because it would perform verification of initial value.

See Office Action at pages 4-5.

Claim 18 recites "the method of Claim 7 further comprising receiving said pseudo-random number generated from said linear feedback shift register, and varying the initial value of said hashing function over time by way of a function operating on one or more variables."

Based on the previous argument provided by the Applicants for Claim 7, Furuta does not teach what is recited in independent Claim 7. Therefore, Claim 7 is believed to contain patentable subject matter. As a consequence, the Applicants respectfully submit that dependent Claim 18, which depends on independent Claim 7, contains patentable subject matter. The Applicants have reviewed Gressel, at paragraphs 0183, 0197, 0372, and 0455, but do not see how these paragraphs teach "varying the initial value of said hashing function over time by way of a function operating on one or more variables," as recited in Claim 18. The Applicants request that the Examiner clearly point out how each and every element of Claim 17 is taught by the cited references. Otherwise, the Applicants maintain that Claim 17 contains patentable subject matter. Since the Applicants believe that the combination of Furuta and Gressel does not teach each and every element of what is recited in Claim 17, the Applicants respectfully submit that a prima facie case of obviousness has not been established. As a consequence, the Applicants respectfully request allowance of the patentable subject matter recited in Claim 17.

CONCLUSION

Based on at least the foregoing, the Applicants believe that Claims 1-22 are in condition for allowance. A Notice of Allowance is courteously solicited. Should anything remain in order to place the present Application in condition for allowance, or should the Examiner disagree or have any question regarding this submission, the Examiner is kindly invited to contact the undersigned at (312) 775-8246.

The Commissioner is hereby authorized to charge any additional fees or credit any overpayment to the Deposit Account of McAndrews, Held & Malloy, Ltd., Account No. 13-0017.

Dated: September 4, 2007

Respectfully submitted,

Roy B. Rhee
Reg. No. 57,303

McAndrews, Held & Malloy, Ltd.
500 West Madison Street, 34th Floor
Chicago, Illinois 60661-2565
Telephone: (312) 775-8246
Facsimile: (312) 775-8100